SPAȚIUL CIBERNETIC - NOUL CÂMP DE LUPTĂ

Victor Adrian Vevera

victor.vevera@gmail.com

Academia Națională de Informații „Mihai Viteazul" Bucureşti

Rezumat: Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă oportunități de dezvoltare a societății informaționale bazate pe cunoaştere, dar şi riscuri la adresa funcționării.

Războiul cibernetic constituie cea mai complexă şi multilaterală formă de atac asupra informațiilor, în vederea dobândirii superiorității informaționale. Scopul principal al acestuia constă în asigurarea separării conducerii centrale a statului, scop vizat de instituții şi cetățeni.

O bună apărare în domeniul cibernetic face ca amenințările să fie gestionabile, în măsura în care riscurile reziduale par în mare parte acceptabile, în mod similar amenințărilor clasice.

Cuvinte cheie: spațiu cibernetic, război informațional, securitate cibernetică, cultura de securitate cibernetică

Abstract: Cyberspace is characterized by lack of physical borders, dynamism and anonymity, generating both opportunities to develop knowledge-based information society, but also risks to its functioning.

Cyberwar is the most complex and multilateral form of attack on information, in order to gain information superiority. Its main goal is to ensure separation of the central leadership of the state concerned institutions and citizens.

Good cyber defense makes the threats to be manageable, to the extent that residual risks seem largely acceptable, similar to those speciffic to the classic threats.

Keywords: Cyberspace, Information warfare, cyber security, the culture of cyber security.

Pe parcursul ultimilor 20 de ani, tehnologia informațiilor s-a dezvoltat deosebit de mult. De la un instrument administrativ pentru optimizarea proceselor de birou, aceasta reprezintă acum un instrument strategic al industriei, administrației şi armatei.

Prin „spațiu cibernetic" înțelegem întreaga lume virtuală (spre exemplu Internetul), în care trebuie să includem şi calculatoarele independente (neconectate cu altele), dar şi fiecare bit de informație existent pe diverse tipuri de medii de stocare: fixe sau detaşabile, fizice sau virtual.

Spațiul cibernetic se caracterizează prin lipsa frontierelor, dinamism şi anonimat, generând deopotrivă oportunități de dezvoltare a societății informaționale bazate pe cunoaştere, dar şi riscuri la adresa funcționării acesteia (la nivel individual, statal şi chiar cu manifestare transfrontalieră).

Alături de beneficiile incontestabile pe care informatizarea le induce la nivelul societății moderne, aceasta introduce şi vulnerabilități, astfel că asigurarea securității spațiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.

Astăzi, spațiul cibernetic reprezintă un larg şi complex câmp de luptă al viitorului, deoarece tehnologia a evoluat foarte mult şi este accesibilă oricui. Iar pentru a preveni sau diminua posibilele consecințe negative avem nevoie, pe de o parte, de implementări de programe care să funcționeze la nivel național şi internațional pentru a reduce riscurile, vulnerabilitățile şi amenințările, iar pe de altă parte se impune o cooperare în domeniu la nivel global.

Actualmente, spațiul cibernetic este departe de a fi doar un spațiu de entertainment. Atunci când vorbim despre domeniul cibernetic, nu ne referim doar la interacțiunile de tip persoană-persoană, navigarea sau trimiterea de e-mailuri, ci şi la interacțiunea dintre cetățeni şi autoritățile publice în interiorul sistemelor de e-guvernare, la comerțul electronic, la sisteme complexe de schimb de date între instituții publice sau private, la informații şi date sensibile cu caracter personal care trebuie să fie protejate.

Ținând cont că „ cine deține informația deține puterea ", este justificată tendința statelor, guvernelor, armatelor, diverselor instituții guvernamentale şi neguvernamentale şi chiar a unor persoane publice sau private de a dezvolta capabilități favorizante culegerii, exploatării şi

transmiterii informațiilor, în vederea realizării scopurilor propuse. În același timp, toate statele și organizațiile, indiferent de tipul acestora, au conștientizat faptul că la rândul lor pot constitui o țintă, respectiv o sursă de scurgere a informațiilor, în situațiile în care nu adoptă un sistem de protecție a informațiilor, bazat pe reguli stricte, proceduri și personal cu expertiză pentru protecția informațiilor.

Informația a căpătat treptat, pe măsură ce era conștientizată necesitatea exploatării ei, o importanță deosebită. Extinderea acestor interese, ale acțiunilor și reacțiunilor în domeniul informațional au condus la apariția unui nou tip de conflict, în plan informațional - războiul informațional - care după unii specialiști posedă caracteristicile războiului clasic.

Războiul informațional, deși este un concept relativ nou, nu este o invenție recentă, forme ale lui (dezinformarea, capturarea solilor, mesagerilor și însușirea informațiilor purtate de către aceștia) fiind folosite, fără a avea o denumire alocată în mod expres, în diverse etape sau evenimente istorice. Deși în aparență respectă principiile unui război clasic, războiul informațional diferă foarte mult de acesta, presupunând folosirea unei arme mai puțin convențională, informația, care, prin folosirea sau nefolosirea ei, poate reprezenta un pericol la adresa securității părții adverse. Acest tip de război vizează în special afectarea opiniei publice, a personalului armatei adverse, reprezentând mai mult o tehnică de slăbire a puterii acestora prin folosirea unor mijloace de influențare psihologică. Specificul acestei noi forme de dezvoltare a conflictului îl reprezintă faptul că se desfășoară subtil, vizând un număr relativ mic de ținte, dar care prin folosirea mijloacelor subversive poate conduce la îndeplinirea obiectivelor și obținerea succesului cu pierderi umane și materiale minime.

În spațiul virtual funcționează rețelele de comunicații și de calculatoare, utilizând produse informatice, care sunt transmise și recepționate prin mijloace de suport fizic și electromagnetic. Astfel, cyberspațiul se întinde de la simplul PC, eventual dotat și cu o cameră digitală de luat imagini, până la uriașele calculatoare ale sistemelor naționale: de apărare, bancar, energetic, transport auto, naval sau aerian etc. Aceste enorme surse de informație, care ar putea fi accesate de la orice calculator personal interconectat la sistem, pun la dispoziția celor interesați un volum de informații atât de variat și de mare, încât modul practic de utilizare a informației accesate nu poate fi nici măcar aproximat și, cu atât mai puțin, evaluat.

Spațiul virtual (cibernetic) reprezintă entitatea integrată global de comunicații și rețele computerizate, programele lor și datele înglobate în ele sau care trec printre diferite părți ale lor. Confruntarea în spațiul virtual este permanentă, se desfășoară mai ales ascuns și subversiv, de regulă în asociere cu componenta informațională și cea psihologică. Efectul cumulat al acestor componente poate înclina decisiv balanța victoriei de partea aceluia care este mai bine pregătit, mai incisiv, care exploatează mai bine oportunitățile, își pune în valoare mai bine punctele tari și își expune mai puțin părțile slabe.

Ținând cont de toate cele menționate anterior, se poate afirma că războiul cibernetic constituie cea mai complexă și multilaterală formă de atac asupra informațiilor, în vederea dobândirii superiorității informaționale. Scopul principal al acestuia constă în asigurarea separării conducerii centrale a statului, scop vizat de instituții și cetățeni.

Securitatea cibernetică reprezintă o parte a securității naționale, în prezent fiind considerată de către multe state și organizații drept o prioritate a securității naționale.

Ca urmare a necesităților societății informaționale, România a investit în ultimii ani în dezvoltarea capabilităților în domeniul securității cibernetice întrucât aceasta a devenit o prioritate a securității naționale. Astfel, în scopul asigurării securității spațiului cibernetic, țara noastră s-a focalizat pe respectarea drepturilor și libertăților omului deopotrivă cu protecția datelor personale. În ceea ce privește stadiul reglementărilor privind zona securității cibernetice în țara noastră, un pas important în acest sens l-a reprezentat aprobarea, în februarie 2013, a Strategiei de Securitate Cibernetică a României de către Consiliul Suprem de Apărare a Țării. Obiectivul principal al strategiei îl reprezintă implementarea măsurilor de securitate care să conducă la o creștere a nivelului de protecție a Infrastructurilor Critice Cibernetice, în concordanță cu noile concepte și politici în domeniu, care au fost elaborate și aprobate la nivel NATO și UE.

Pe de altă parte, nu este suficient să avem o lege a securității cibernetice, ci ar trebui elaborat şi adoptat un set de standarde în domeniu. Toate Infrastructurile Critice Informaționale (deopotrivă publice şi private) trebuie să beneficieze de minime politici de securitate şi praguri critice cu rolul de a preveni sau cel puțin pentru a limita efectele atacurilor cibernetice, de la cele mai puțin semnificative la cele de nivel mediu.

Cultura de securitate cibernetică reprezintă un factor important în societate şi ca atare este necesar ca instituțiile statului să-şi concentreze eforturile în vederea creşterii nivelului culturii de securitate în România. Societatea civilă trebuie să înțeleagă că are deopotrivă şi responsabilitatea asigurării securității spațiului digital, şi că este necesar să existe din partea acesteia deschiderea către cooperare cu instituțiile care au responsabilități în domeniu.

Trebuie de asemenea, subliniat rolul important al educației în orice societate. Educația în zona deprinderilor utilizării mijloacelor de asigurare a securității cibernetice este doar la început, însă statele trebuie să se concentreze pe această latură a securizării spațiului virtual şi să investească din ce în ce mai mult pentru a construi cu succes programe inovative. Trăim într-o eră informațională, în care internetul a devenit tehnologia hotărâtoare, iar nevoia de personal cu expertiză în domeniul securității cibernetice este acută. Ca atare, nu există nici o îndoială că trebuie accelerat procesul de învățare şi de dezvoltare a abilităților utilizatorilor de internet.

România continuă dezvoltarea programelor educaționale şi a instruirii profesionale pentru a crea suficienți experți care să răspundă provocărilor actuale. În vederea îmbunătățirii măsurilor de securitate cibernetică, investițiile şi acțiunile trebuie prioritizate de către guvern şi organizații.

Dacă luăm în considerare factori precum: caracteristicile internetului văzut din perspectiva unui sistem global de informare, atacurile cibernetice care se pot manifesta fără frontiere, reiese necesitatea cooperării regionale şi internaționale în domeniul securității cibernetice. Problema principală referitoare la cooperarea pe teme de securitate cibernetică, o reprezintă abordările diferite ale statelor: fie prin prisma securității naționale, a drepturilor omului sau a intereselor economice. România este implicată în numeroase activități de cooperare în domeniul securității cibernetice, atât cu state ale Uniunii Europene, cât şi cu state membre NATO.

Crearea şi dezvoltarea de parteneriate publice-private reprezintă de asemenea, o necesitate având în vedere că securitatea cibernetică este atât responsabilitatea guvernelor, prin serviciile de informații şi instituțiile de aplicare a legii, cât şi a sectorului privat. Ca urmare, este necesar să fie stabilite mecanisme de cooperare între sectorul public şi cel privat în scopul prevenirii, identificării, analizării şi reacției la evenimente de natură cibernetică. De asemenea, trebuie considerată o necesitate împărtăşirea cunoştințelor şi bunelor practici ca o modalitate de sporire a capabilităților de asigurare a securității cibernetice.

Asigurarea securității cibernetice se bazează pe cooperarea la nivel național şi internațional pentru protejarea spațiului cibernetic, prin coordonarea demersurilor naționale cu orientările şi măsurile adoptate la nivel internațional, în formatele de cooperare la care România este parte.

Având în vedere dinamismul evoluțiilor globale în spațiul cibernetic, precum şi obiectivele României în procesul de dezvoltare a societății informaționale şi implementare pe scară largă a serviciilor electronice este necesară elaborarea unui program național detaliat, care - pe baza reperelor oferite de prezenta strategie - să asigure elaborarea şi punerea în practică a unor proiecte concrete de securitate cibernetică.

Până în prezent, cei mai periculoşi actori în domeniul cibernetic sunt tot statele-națiuni. În pofida unor capabilități ofensive aflate din ce în ce mai mult la dispoziția rețelelor criminale care ar putea să fie folosite în viitor şi de actori non-statali precum teroriştii, spionajul şi sabotajul de înaltă sofisticare în domeniul cibernetic, aceştia au în continuare nevoie de capabilitățile, hotărârea şi raportul cost-beneficii ale unui stat-națiune.

O bună apărare în domeniul cibernetic face ca aceste amenințări să fie gestionabile, în măsura în care riscurile reziduale par în mare parte acceptabile, în mod similar amenințărilor clasice.

BIBLIOGRAFIE

1. **ALEXANDRESCU, C.; ALEXANDRESCU, G.; BOARU, GH.:** Sisteme informaţionale – servicii şi tehnologie. Editura U.N.Ap. „Carol I", Bucureşti, 2010.
2. **FRUNZETI, T.; MUREŞAN, M.; VĂDUVA, GH.:** Război şi haos. Editura Centrului Tehnic -Editorial al Armatei, Bucureşti, 2009.
3. *** Strategia de Securitate Cibernetică a României
4. www.securitatea-cibernetica.ro
5. www.cert.org
6. www.europa.eu